Cybersecurity 2021 Special Report
Table of Contents

Introduction .................................................................................................................................................... 3
Looking Ahead to 2022: The Cybersecurity Landscape for the Legal Industry .................. 4
Egress ...................................................................................................................................................................... 7
iManage ................................................................................................................................................................ 11

About


Legal Tech Publishing is highly recognized for its publications, educational webinars, case studies, and whitepapers.

Subscribe to receive updates and free resources:

info@legaltechpublishing.com

LegalTechPublishing.com
Welcome to Legal Tech Publishing’s 2021 Cybersecurity Special Report
By: Cathy Kenton and Brian Dalton

If you’re like most lawyers, your response to ever-increasing cybersecurity risk is simple: nothing.

You may think your small firm will fly under hackers’ radar. Or, you might note that even large companies are regularly victimized and conclude that there’s no chance your firm will succeed where these institutions have failed.

But, as a growing cohort is learning the hard way, this approach is courting disaster.

The good news is that you’re reading this right now, which means you’re already ahead of the game.

Still more good news: setting up a cutting-edge system has become surprisingly painless.

In this special report on the state of law firm cybersecurity, we’re pleased to present a 2022 outlook from renowned cybersecurity analyst and professor Leeza Garber.

And later, the top companies in tech show how you can keep your firm safe amid these ever-changing threats.

Here’s to shoring up your firm — which may well be among the most important professional actions you’ll ever take.

To your success,

Cathy Kenton, CEO, Legal Tech Media Group/Legal Tech Publishing

Brian Dalton, SVP, Breaking Media
Looking Ahead to 2022: The Cybersecurity Landscape for the Legal Industry

By: Leeza Garber, Esq.
November 2021

Leeza Garber Esq. is a cybersecurity and privacy lawyer; award-winning lecturer at The Wharton School; adjunct professor at Drexel University’s Kline School of Law; and her book Can, Trust, Will.: Hiring for the Human Element in the New Age of Cybersecurity is being published by Business Expert Press and is available for pre-order now.

Hackers have been successfully targeting law firms for years. Malicious actors have held practices for ransom over and over again, blackmailed attorneys (and their high profile clients), and breached their vendors, all through cyberattacks. The statistics continue to illustrate an increasing number of law firms reporting security breaches while other reports focus on those that show signs of compromised networks. As 2021 draws to a close and cybercriminals look ahead to 2022, law firms have no choice but to acknowledge these increasing threats and the necessity to not only employ proactive cybersecurity measures but to fully analyze and understand the methods and origins of why their practices are under attack. The coming year promises cutting-edge technology to assist in finding, connecting with, and managing clients, providing more efficient data management and cloud-based services, and improving work-from-home structures and platforms as the pandemic continues to impact legal practices — and all major industries — around the world. But with these new opportunities come more points of vulnerability. Thus, governments and other regulatory bodies are proposing legislation attempting to guide law firms to protect their valuable digital assets. Bar associations and other powers-that-be struggle to assist during the limbo period as the law plays its eternal game of catch-up with technology.

Legal technology comes in all shapes and sizes, catering to entities ranging from solo practitioners to Biglaw to corporate legal departments, and for needs that span a range of eDiscovery to client communications to cloud-based data storage. And the tech just keeps getting consistently better and faster. Whether a firm has developed a customized solution with in-house programmers or purchased and adapted a vendor’s offering, technology continues to evolve in positive ways. This progression has worked miracles amid the ongoing pandemic, as lawyers have been able to maintain busy schedules through high-definition remote video meetings with their clients, judges, and fellow practitioners (sometimes as a cat or otherwise).

As 2022 draws near, more high-tech options will become a reality for lawyers seeking new methods for networking and conferencing remotely with clients. Just as 2021 saw Facebook change its parent company name to Meta, virtual reality will become a real option for remote meetings; in fact, one Biglaw firm has already released their own lawyer’s guide to the metaverse. While internet-connected watches, speakers, printers, cameras, and refrigerators are commonplace ways for attorneys to stay glued to their work, more will be sporting smart Ray-Bans to instantaneously and seamlessly connect via video chat, potentially even entering their avatars into a new digitized universe to discuss litigation strategy.

Even if your practice has its C-Suite execs and IT teams dedicated to vetting new software and updating operating systems, it may not be enough. That should be a warning call to small and mid-size law firms and in-house counsel for companies smaller than the Fortune 500. Proper vetting procedures require verification and validation of your vendors’ cybersecurity best practices — and the cyber supply chain can be larger than appreciable at first blush. Only twenty-three percent of law firm and legal organization employees recently surveyed were aware of a formal process in place at their organization to evaluate legal technology. However, eighty-five percent responded that they rely on legal technology to improve productivity.

Every piece of tech that touches personally identifiable information (PII) must undergo this strict auditing procedure. The first step is to identify what information the law firm possesses, where it is located, who (or what program) has access to it, and why access has been granted — what cybersecurity pros call “analyzing the data flow.” Only then can a true risk analysis be completed and shiny new gadgets and software considered. It’s not just the exciting gadgets that need careful review; the unglamorous need special attention too. Law firm file transfer platforms, cloud storage, and human resource and payroll services (both relative unknowns and household names) continue to fall victim to cybersecurity crises.

As we close out the year 2021, it is certainly not a valid excuse for a law firm to claim...
that it was unaware of how a particular app, platform, smartwatch, or server handled information security. Reasonable efforts to protect client data are essential to the practice of law, which means understanding the tech in place and what threat vectors exist and are on the horizon. Technological competency is not only a requirement — as dictated by the American Bar Association and certain state bar associations — but it’s simply good business. Data breaches are expensive and embarrassing; as of September, Texas adopted legislation requiring the state AG to publish a data breach wall of shame. Other states are considering following suit.

The cyberthreats we continue to read about in daily news headlines, such as phishing attacks and ransomware, persist in the law firm environment. The vulnerabilities involved, including unpatched software, recycled passwords, and haphazardly disabling or neglecting to enable security features like dual-factor authentication, are far too often easily avoidable. These attacks and points of exposure may take different forms but are ultimately the evolution of basic breach concepts and mechanisms. However, a few noteworthy updates to the hacker’s repertoire will be in heavy rotation come 2022. This past year saw the rise of double extortion ransomware, which not only encrypts a system until a ransom is paid but also exfiltrates data for potential blackmail purposes. While many of the publicized cases of double extortion ransomware date back to 2020, ongoing investigations will highlight more recent incidents as law firms undergo the necessary digital forensic investigation process.

In addition, distributed denial of service (DDOS) attacks, which send overwhelming traffic to an online service in an attempt to cause a malfunction and make it unavailable, have been hitting major providers (read: Amazon, Google, and Microsoft) in higher numbers in recent months. And large-scale content delivery network (CDN) outages and domain name system (DNS) attacks, which — put very simply — compromise the connection to websites, have become commonplace. These often-overlooked threat vectors can cause an aspect of a firm’s website or another client-facing service to go dark for hours at a time. While law firms cannot proactively fight this type of hack (unless they own the affected server/service/network/system), they should be aware of the potential aftershock and be able to respond quickly to suspended business operations.

While not as exciting as malicious hackers, internal threats deserve mention. As many law firms maintain a remote workforce or hybrid option, the boundaries between work life and personal life continue to blur, leading to an (even more) overworked, exhausted, shouldn’t-have-clicked-on-that-link group of attorneys. Cybersecurity awareness training is a must, and 2021 showcased notable developments in companies offering phishing testing and tabletop exercises, amongst other gamified educational activities. It is worth noting that in 2022, more serious cybersecurity education could become mandatory, as the New York State Bar Association ponders a cybersecurity CLE requirement. That could improve the information security of the legal sector significantly, as fifty-one percent of law firm and legal organization employees believed that a lack of tech-savvy users was a significant barrier to the use of legal tech in general. Until such education becomes required, there is no reason why attorneys shouldn’t take advantage of opportunities to choose a cybersecurity CLE course offering or even take thirty minutes to watch a cybersecurity vendor’s free presentation on newsworthy threats. In a larger firm setting, it’s also a good idea to set up panel discussions with in-house security experts — such as the chief security officer, chief information security officer, IT or privacy lead — to review best practices, existing security protocols, and tech upgrades.

Work-from-home environments require special care on the technology front. 2022 will see a continuing array of cybersecurity threats, including the potential for unwelcome viewers and listeners via Internet of Things devices, along with vulnerabilities stemming from unpatched systems and creative loopholes in best practices (for example, those devised to provide senior partners the convenience of circumventing extra security steps). At the beginning of the pandemic, the Pennsylvania Bar Association released enhanced guidance surrounding ethical obligations for lawyers working remotely. That included detailing necessary precautions when discussing client-related matters in front of smart devices that record and even employ AI to transcribe and review those recordings for the accuracy of their technologies. Unfortunately, the statistics do not look promising: a recent survey found that only thirty-eight percent of U.S. office workers received additional training on protecting their work-from-home setups. In comparison, eighty-seven percent of IT teams believe security has taken a backseat to business continuity during the pandemic. That is ironic considering many cyberattacks aim to and succeed in disrupting daily workflow.

As of the writing of this article, there is still no holistic federal law regarding cybersecurity or privacy — though strong federal protections of health information and financial data may apply to law firms, depending on the content and client-base, and the nature of data collected by the practices. However, many State lawmakers continue to raise the bar in terms of the ways private data must be protected by businesses — including, of course, law firms. New York, Connecticut, and North Dakota recently created stricter obligations for how and how quickly to report data breaches, along with increased financial penalties and more demanding remedial requirements. Other states will likely follow suit. Especially after the game-changing California Consumer Privacy Act (CCPA) sets its teeth in, with 2021 highlighting one of the first CCPA-based class actions to end in a multimillion-dollar settlement for data breach victims due partly to the defendant’s failure to implement reasonable security procedures.

In fact, in 2021, approximately forty-five States proposed 250 pieces of legislation related to cybersecurity. These ranged from recognizing cybersecurity awareness month to the establishment of comprehensive information security programs. In addition, nearly twenty cybersecurity bills have been put forward in Congress. These include a cyber reporting bill that would require faster breach disclosure and notification processes and a ransom disclosure act that would force victims to detail the circumstances surrounding a ransomware attack, including whether they ultimately paid a ransom. Some bills failed, some were enacted, and others are still under consideration; some are simply minuscule amendments to existing legislation, while some contemplate more significant obligations. Some of the bills would inevitably impact law firms if passed — even if just through a trickle-down effect. While political agendas and bureaucratic procedures will tie up many of these proposals during the year to come, 2022 will certainly see even more legislative attention to cybersecurity. Increased cybersecurity-related proposals and enacted laws will emerge in the context of major antitrust and privacy actions against big tech, federal government cybersecurity budget demands, and executive actions requesting public-private partnerships to fight cybercrime.

Lawyers’ ethical obligations to their clients related to cybersecurity are also escalating — and will only increase in the coming year. Guidance regarding confidentiality, security of information, and obligations after a data breach or cyberattack have been pillars of the attorney-client relationship for years.
However, what is considered “reasonable competency” in terms of a lawyer’s knowledge and understanding of the technology they choose to use continues to evolve upwards. But it is clear that most consider the end goal to be a worthy endeavor: seventy-nine percent of recently surveyed law firm and legal organization employees believe that the use of legal technology has increased the quality of the work product of their respective organizations over the past year, and such benefits deserve due attention.

Best practices do not simply mean having an IT person on call. The concept of cyber hygiene refers to the use of encryption, complex passwords, antivirus and antimalware software, and other basic proactive cybersecurity practices. It also encompasses the obligation to stay on top of threats, maintain business continuity in an internet-based world, and appreciate why security measures — like the extra ten-second “annoyance” of using dual-factor authentication — are necessary to the practice of law right now. And as the legal world moves ahead into 2022, adopting exciting new technology must be done alongside the implementation of cybersecurity measures and an appreciation of expanding points of vulnerability.
Egress Preven...act as a shield to prevent human errors. It minimizes people emailing data to the wrong recipient or sharing the wrong sensitive attachment.”

Company Name Brand
Egress Software Technologies Ltd. (UK)
Egress Software Technologies Inc (US)

Product Name Brands
Defend, Prevent, and Protect

Latest Developments and Roadmap
• Egress added the Defend module to its Intelligent Email Security platform to stop bad actors from executing a successful phishing attack.
• Prevent and Defend modules will soon communicate with each other to identify and mitigate security threats to email.
• Like the Protect module, Prevent and Defend will have self-service licensing options.

Human Error – Awareness and Prevention
A 2021 survey of 500 IT leaders and 3,000 employees in the US and UK across various industries, including legal, revealed that 94 percent of organizations experienced insider data breaches. Human errors led to the most severe incidents. The survey showed that IT leaders were most concerned about malicious insiders. Almost three-quarters of the organizations surveyed were victims of phishing attacks and acknowledged data breaches from employees violating company policies.

Because people in organizations that share content via email get hacked, make mistakes, and break the rules, Egress developed a platform to protect law firms from their most significant vulnerability— inbound and outbound threats to email. The company categorizes these threats into three areas and addresses each with a particular module or product.

Defend protects a law firm from inbound attacks emanating from incoming mail,

Figure 1: The Egress Defend module provides detailed information on phishing threats in email.
such as phishing. Prevent stops people from sending an email or attachment to the wrong recipient or exfiltrating client data for personal use. Protect applies the appropriate level of security to email through encryption.

**Defend – Advanced Phishing and Threat Detection**

Egress Defend applies a zero-trust model to all incoming emails protecting users from phishing. Defend can identify if a subject line changes in an email thread or if any email seeks financial data.

The Defend module displays “heat-based” color-coded banners in an email when it identifies or suspects phishing. Red banners indicate high confidence of phishing; amber banners indicate a user should exercise caution and further examine a message to confirm or deny phishing; blue banners display informational messages, warning a recipient that a message is from an outside domain, first-time sender, or may include financial or sensitive data.

Users can click the banners for more detailed information on the message along with Defend's analysis. These real-time teachable moments provide users with active learning that builds up their security awareness and transforms them into the first line of defense against attacks. See Figure 1 on the previous page.

**Prevent – Manage Human Error**

Egress Prevent acts as a shield to prevent human errors. It minimizes people emailing data to the wrong recipient or sharing the wrong sensitive attachment.

Deploy Prevent in Outlook via a plug-in where it reviews all of a user’s sent mail to analyze behavior, such as what mail goes to whom and the types of content. The plug-in securely communicates with Egress's risk application programming interface and machine learning, based in the Microsoft Azure cloud.

Prevent performs a risk assessment on a user’s emails based on what normal looks like for them. The Egress ribbon tab in Outlook includes a shield icon that operates as a traffic light for outgoing emails. Green means good to go, orange represents a potential risk to review, and red indicates you should not send an email. If a user includes someone who is not usually a recipient, the shield turns color in real-time. Click on the shield, and a panel opens to explain the warning code. See Figure 2.

If you continue to send an email despite the warning, a window pops up with a reminder that you wouldn’t typically include the recipient with others in the To field.

Prevent pays attention to the type of content sent to clients and domains. When sending a client email with attachments,
Prevent scans the content of messages and attachments and gleans matter or client identification numbers. Over time, it learns the content clients receive. If a user makes a mistake by selecting the wrong client attachment, Prevent will warn, “you wouldn’t normally send [Matter ID] to [recipient]; are you sure you want to send?”

A law firm can create static rules in Prevent to protect users from delivering content to the wrong recipients. You can associate keywords with specific email domains. If Prevent sees a keyword in content going to an unknown domain, it will prompt the sender to verify the email and attachment before sending. Note that Prevent can stop the email and not simply warn the sender.

Prevent can also protect a law firm from data exfiltration and detect phishing attempts. Suppose partners or associates send copies of emails or client lists to personal email addresses. In that situation, Prevent can reroute the mail to a moderator’s email inbox for them to approve or reject transmission. And when bad actors masquerade as good, Egress’s domain hygiene service can ensure users don’t fall prey to phishers and communicate with the right people.

**Protect – Secure Email and File Transfer**

The Egress Protect button on the Egress ribbon tab in Outlook displays levels of protection available for email. Out of the box, labeled protections include unprotected, confidential, restricted, and secret. The default option, Unprotected, applies no encryption for an email with non-sensitive information. Select Confidential to encrypt email at the transport or message level. For Restricted and Secret emails, Protect encrypts the email and any attachments. See Figure 3.

Authenticated recipients can view, copy, and save a restricted email, but they cannot save, print, or copy and paste. Egress can detect sensitive information and suggest or enforce a level of protection.

Recipients receive restricted and secret emails via a notification from Protect. The information includes a one-click action to access the message on Egress’s platform without entering a username and password. But if the recipient wants to reply, they must set up credentials on the platform. Egress provides support when recipients forget their username and password.

Protect can also send large files exceeding Outlook’s send limits. Protect copies the files on the local machine, encrypts them, and sends the recipient a one-click notification to access them on the Egress platform.

**Integration, Configuration, and Branding**

The Egress platform and its three a la carte modules work with Office 365 in on-
premises, cloud, or hybrid mode. A law firm can customize the modules down to the user level. The user experience includes a plug-in for Outlook on the desktop, online, and mobile devices (Android and iPhone).

Law firms can configure Egress modules to match their email security policies. They can also apply their brand to user interfaces.

**Pricing**
Software-as-a-Service (SaaS) a la carte subscription prices for Egress Prevent and Defend are per user per year, starting with fifty users. **Egress Protect supports self-service, per-user licensing for 1-25 users.** For more than twenty-five users, contact Egress. The company is exploring a self-service licensing model for Prevent and Defend.

Who is Egress?
In 2007, John Goodyear, Neil Larkins, and Tony Pepper launched Egress in London to protect digitally shared information after working together at an endpoint data security company, Reflex Magnetics, which Checkpoint Software Technologies acquired. Since Egress launched its first product, Protect (encryption), in 2010, it has been on a growth trajectory. It received $2.8M in venture capital from Albion VC in 2014, and following the launch of Prevent in 2016, Egress received $40M in Series C funding from FTV Capital and Albion VC. This year, the company launched Defend after **acquiring the technology from Aquilai.** The company has more than 250 global employees.

Why Buy Egress email security products?
• Real-time protection to securely share and prevent client data from unauthorized access.
• Zero-trust analysis of incoming email to defend against phishing and ransomware attacks.
• Easily protect email with levels of encryption matching data sensitivity and privacy.
• A la carte modules offer predictable pricing models.

Try Egress Today!
**Contact Egress** for more information on Prevent and Defend. Start a 14-day free business trial of Egress Protect before you buy.
iManage Tools Help You Minimize Threats and Manage Security, Risk Mitigation, and Information Governance

“iManage Security Policy Manager utilizes need-to-know (NTK) methodology with access provided or denied based on its use for matters, clients, practice group teams, ethical walls, email policies, and legal holds (new).”

Company Name Brand
iManage

Product Name Brands
Threat Manager, Security Policy Manager, Records Manager

Latest Developments and Updates
- Security Policy Manager updates include added support for practice group and departmental security; introducing legal hold capability; and support for additional systems including Elite 3E, Aderant, SharePoint, and (shortly) Teams.
- Threat Manager updates include a new classification-based approach with automated actions to neutralize threats; the Threat Manager robot interprets past anomalous behavior more intelligently, resulting in greater alert accuracy when monitoring users who have given notice.
- Records Manager updates include the introduction of a web client for end-users; key metrics for records managers, delivered via dashboards; and enhanced disposition capability.

Taking Steps to Protect Your Data
Adapting to perpetual changes in the frequency, volume, and scope of Cybersecurity threats keeps anyone managing (or using) technology constantly on the lookout. iManage has five applications in its suite of Security Risk Mitigation to help you reduce risk and keep your sensitive data protected. They include the following:
- Business Intake automates all processes through the lifecycle of clients/matters.
- Conflicts Manager identifies and clears conflicts.
- Security Policy Manager segregates information and enforces need-to-know (NTK) access and ethical walls.
- Threat Manager detects unusual or questionable behavior from internal or external threat actors and takes action to neutralize threats and prevent data loss.
- Records Manager supports the defensible disposition of content for both electronic and physical data. Integration with external data warehouse management tools is supported, including Iron Mountain and O’Neil.

Figure 1: The Security Policy Manager Dashboard provides one interface designed for administrators and security delegates. Users will see only clients/matters assigned to them, whereas administrators will see everything in the system.
All five of these applications aid clients in managing risk throughout the lifecycle of a matter from pre-intake through matter (or client) closure and disposition of electronic and physical records. This review covers Security Policy Manager (SPM), Threat Manager (TM), and Records Manager (RM).

**Security Policy Manager**

iManage Security Policy Manager utilizes need-to-know (NTK) methodology with access provided or denied based on its use for matters, clients, practice group teams, ethical walls, email policies, and legal holds (new). See Figure 1 on the previous page.

SPM utilizes agents to perpetuate security and supports Windows file shares, all major time entry systems, iManage Work, SharePoint (Teams coming soon), as well as client-customized agents for other applications.

Clients can be open or restricted, and if a client is restricted, all its associated matters will be as well. Restrictions can also be made at the matter level and will only be visible to that matter team. If a matter is open, it can have exclusions applied, such as conflict of interest information.

Click on a matter to see its details, including an overview, general information, security, staff, notifications, conflicted users, opposing team sets, and locations. You can add staff or groups by clicking the blue Add Member button or the gear icon to access self-maintaining rules. Use those rules to automate adding users to a matter or leverage billing activity or document activity.

Access SPM legal holds in the left navigation panel to create a hold, add clients, matters, and custodians, and set up scheduled notifications. Custodians can be added individually or via self-maintaining rules. Hold details show all items and custodians on hold. There are plans to develop additional legal hold functionality such as questionnaires and managing responses.

You can create ethical walls through Opposing Team Sets, including multi-sided objects that ensure ethical walls between opposing sides. For example, if the firm represents multiple hotel chains competing to purchase a property, barriers are put in place between each hotel chain to maintain confidentiality.

Should a user need access to a restricted matter, access can be provided for a limited period via email approval by a delegated administrator, or IT can grant greater access.

** Threat Manager**

iManage Threat Manager detects both internal and external threats to the system. iManage Threat Manager uses work audit logs to analyze everything a user does and builds a “fingerprint” for each user.

**Figure 2**: The Threat Alert Dashboard shows alerts for each user. Highlighted items are a clickable entry point to show the details of an alert and the impacted documents.
uses work audit logs to analyze everything a user does and builds a “fingerprint” for each user. TM can identify aberrant activities and flag them for review or immediate action by using artificial intelligence (AI) and machine learning (ML) to look back over time. See Figure 2 on the previous page.

The TM left navigation panel presents the security team with options for detect and protect, behavior analytics, matter activity, compliance, and outliers for general analysis.

The detect and protect feature is all about identifying and guarding against well-known patterns or risks and initiating action that prevents data loss. When detect and protect criteria are met, action can be taken; available options include notifying the compliance team, warning the end-user, and disabling an account. For example, a rule warning a user when twenty-five documents are exported and disabling an account when activity persists.

Behavior analytics rules are designed to be early indicators of potential risk by detecting differences using user behavioral modeling and providing an alert when a user exhibits a different behavior from a peer group or individual norm. Click on a behavioral analytics alert to see a risk score and show the count, group mean and threshold, individual mean, threshold, and standard deviation. For example, a user may have an exceptionally high export count of over one thousand documents, while they usually only export about thirty, and their peers only typically export five. TM will show a list of all documents accessed when that alert was activated, including document metadata and the public-facing IP addresses used when the trigger event occurred.

Matter activities present insight into who has access to the matter and what they are doing. The security team has visibility into all activities, including the number of documents created, exported, emailed, printed, viewed, opened, closed, copied, or modified. Each of these numbers is a clickable entry point and will display an associated list of documents.

Compliance reporting looks at all users and identifies who is not engaging the system as required, such as the user with the fewest number of documents and emails. Non-filing could represent a risk to the organization and indicate that data may be stored in an unauthorized and unsecured location.

Records Manager iManage Records Manager has been around for over twenty-five years delivering integrated electronic and physical records management and

![Figure 3: The Records Manager Dashboard gives users a clear picture, with metrics, on the status of what is in the system and what is in the queue for disposition.](image-url)
buyout from HP in 2015, and the company settled into its headquarters in Chicago, Illinois, with approximately 150 employees. iManage has grown to over 750 employees who support more than 2,500 of the largest law firms and more than 1,200 corporate enterprise and legal customers, including more than one hundred of the Fortune 500 worldwide.

Why Buy iManage Security Policy Manager, Threat Manager, and Records Manager?

• Security Policy Manager is built into the fabric of the platform and is scalable. Users can see policies, understand limitations of access, and remove bottlenecks granting access via delegates. SPM supports Windows File Shares, SharePoint 2016/2019, Teams (coming soon), Elite 3E, Elite Enterprise, Aderant Expert, Carpe Diem, Intapp Time and Open, and iManage Work and Records and Conflicts Manager.

• Threat Manager provides fewer false positives through user/entity behavior analytics powered by machine learning and guards against malicious insiders—even low intensity. TM quickly determines if an alert is real or not via advanced forensic investigation capability and uses compliance reports to detect users that are not using the system.

• Records Manager provides central retention policy definitions for both physical and electronic records. RM offers a single interface for end-users and records managers via seamless integration with iManage Work and manages data in place with no need to adjust workflow.

Pricing

iManage prices its Security, Risk, and Governance solutions as a per user per month subscription, delivered as part of solution bundles on their core document and email management platforms.

Who is iManage?

iManage was founded in 1995 and delivers on-premises and cloud-based services spanning document and email management, contract intelligence, records management, governance, and security for law firms and corporate law departments worldwide. After several mergers and acquisitions, the iManage leadership executed a management
Thank you for reading, let’s keep in touch!

We appreciate the time you spent researching solutions for your law firm. New products, feature updates, and announcements happen throughout the year. So, to help you stay informed we have expanded Legal Tech Publishing’s Buyer’s Guide Series to include an eBook for nearly every product category. Subscribe to receive notifications when a new guide is released. Follow us on the channels below for updates and special virtual events.

Subscribe to our Vimeo Channel

Follow us on Twitter

Like us on Facebook

Follow us on LinkedIn
This buyer's guide is supported by vendor sponsorships. The products and services selected for the guide are done at the author's discretion. Reviews are also written to reflect the opinion of the author. Each product or service must first be selected for the guide, then invited for inclusion before sponsorship is requested. Additionally, emerging technologies who do not have funding to pay for sponsorship are included based on the level of value they offer to law firms. All sponsorship proceeds go towards the costs associated with the production and distribution of the guide.